National Infrastructure Protection Center
NIPC Daily Open Source Report
for 07 January 2003

Current Nationwide
Threat Level is

ELEVATED
SIGNIFICANT RISK OF
TERRORIST ATTACKS

For info click here
www.whitehouse.gov/homeland

Daily Overview

- Reuters reports Saudi Arabia and Russia, agreed today to keep their oil supplies flowing to world markets in a bid to control prices that could jeopardize global economic growth. (See item 3)

- The Associated Press reports PRG Packing Corp is recalling 26,400 pounds of chicken frankfurters because they may be contaminated with listeria. (See item 15)

- Computerworld reports the Center for Strategic &International Studies asserts that computer networks and critical infrastructures are distinct entities and that the threat from cyberterrorism is far less serious than the government and the media contend. (See item 23)

- The New York Times reports experts are concerned that as American companies increasingly move their software development tasks out of their own offices to computer programming companies here and abroad, there are new concerns about the security risks involved. (See item 25)

- Editor's Note: The NIPC Daily Open Source Report is now being published in PDF format. The reader is free and can be downloaded from http://www.adobe.com/products/acrobat/readstep2.html.

- Editor's Note: The NIPC Daily Open Source Report is now aligned to cover the critical infrastructure sectors as identified in the National Strategy for Homeland Security. Currently covered sectors, which were set forth in Presidential Decision Directive 63, are included in the new format. The new Sector alignment is as follows: Agriculture, Food, Water, Public Health, Emergency Services, Government, Defense Industrial Base, Information and Telecommunications, Energy (to include Electric Power, and Oil and Gas), Transportation, Banking and Finance, Chemical Industry and Postal and Shipping. Readers wishing to comment on the contents or suggest additional topics and sources should contact Melissa Conaty at 202–324–0354 or Kerry J. Butterfield at 202–324–1131. Requests for adding or dropping distribution to the NIPC Daily Open Source Report should be made through the Watch and Warning Unit at nipc.watch@fbi.gov.

Energy Sector

Current Electricity Sector Threat Alert Levels: <u>Physical</u>: **Elevated,** <u>Cyber</u>: **Elevated**
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES–ISAC) – http://esisac.com]

1. _January 06, Atlanta Journal–Constitution_ — **Marketers raise natural gas prices.** Georgia's two top natural gas marketers, citing a surge in wholesale prices, Thursday announced hefty price increases for residential consumers. **Georgia Natural Gas Services said its variable prices, subject to monthly fluctuation, are 16 percent higher than in December, while Scana Energy announced an 11 percent increase.** Georgia Natural Gas, which has 550,000 customers, and Scana, which supplies 400,000 homes and businesses, together serve more than 60 percent of the state's deregulated natural gas market of 1.4 million homes and businesses. Spokesmen for Georgia Natural Gas took great pains to say Georgia's 4–year–old natural gas deregulation is not to blame. "These wholesale price increases are impacting natural gas companies nationwide and therefore will affect natural gas consumers throughout the United States," said Mike Braswell, the No. 1 marketer's chief operating officer. **Robert Baker, chairman of the Public Service Commission, said rising gas prices could tax the ability of many consumers to pay their bills and precipitate cutoffs of service. He faulted marketers for not locking in wholesale prices when they were low earlier in the year. That would have "eliminated or greatly minimized the need for any rate increases" for consumers, he said.** The price increases are "definitely a cause for concern," said Kristy Holley, the governor's consumer utility counsel. She said prices have not declined much during the past year, "and now we don't expect much this winter." **Wholesale natural gas prices soared 9.7 percent, the biggest gain in more than eight months,** Thursday on expectations that subfreezing weather forecast for much of the nation will strain supplies of the fuel, Bloomberg News reported. Source: http://www.accessatlanta.com/ajc/business/0103/03gas.html

2. _January 06, Star–Telegram (Texas)_ — **Chill heats up natural gas futures. Predictions of more cold winter weather pushed natural gas futures prices up 9.6 percent Thursday in trading on the New York Mercantile Exchange.** The February contract for natural gas delivery rose by 44.1 cents to $5.23 per million British thermal units. Futures prices have risen by 14 percent in the last month and 86 percent in the last year. The spot price for next–day delivery of natural gas in the Southwest was quoted at $4.97 per million British thermal units, up 8.3 percent from Tuesday's close. **Analysts say that U.S. supplies are tighter because of reduced production, and also because of the threat of colder–than–usual winter weather**

after relatively mild temperatures the last two years. The onset of cold weather will hit as U.S. inventories of natural gas are down 5.2 percent from a week ago and 19 percent from last year, according to the U.S. Energy Department. A new inventory report will be issued Friday morning. The reductions in supplies reflect continued high demand during 2002 while natural gas production fell by 1.6 percent, compared to a 2.4 percent increase in production during 2001.
Source: http://www.dfw.com/mld/startelegram/4861356.htm

3. *January 06, Reuters* — **Saudi Arabia and Russia agree to manage oil prices. The oil−producing giants, Saudi Arabia and Russia, agreed today to keep their supplies flowing to world markets in a bid to control prices that could jeopardize global economic growth. The meeting in Riyadh of the world's top two oil exporters came as prices soared amid fears that a war in Iraq could disrupt exports throughout the gulf and as a strike in Venezuela threatens supply in the United States.** "Both sides discussed the importance of stabilizing oil prices," the Saudi oil minister, Ali al−Naimi, said, and the need to keep those prices from rising to the point where they could hurt global economic growth. "The kingdom and Russia agree that cooperation is necessary to ensure that there is no lack of oil supplies," al−Naimi said after meeting with the Russian energy minister, Igor K. Yusufov. **For its part, OPEC is set to raise output quotas in mid−January by up to one million barrels a day, the organization's president, Abdullah bin Hamad al−Attiyah, said today.** Russia's oil output is set to rise to an average of 8.4 million barrels a day this year, up 800,000 barrels a day from 2002. **Analysts say Russia could easily turn up the taps by an additional two million barrels a day over the next few years and overtake Saudi Arabia, which was pumping a touch more than eight million barrels a day in the latter part of last year.**
Source: http://www.nytimes.com/2003/01/06/business/worldbusiness/06OPEC.h tml

4. *January 04, Seattle Post−Intelligencer Reporter* — **Heavy rain and high tides have battered the Washington coast and flooded homes in low−lying areas, while high winds caused thousands of power outages in the northwest portion of the state.** The weather knocked out power to more than 30,000 Puget Sound Energy residents in four counties about midnight Thursday. Although the power had been restored in Whatcom, Skagit and Island counties by about noon yesterday, 30,000 Kitsap County residents were still without electricity. Puget Sound Energy spokesman Tim Bader said the company hoped to restore power to Kitsap by yesterday evening after several damaged transmission lines in remote areas were fixed. The state Department of Transportation was closely monitoring roads throughout the region yesterday, a day after about a foot of standing water prompted a nine−hour shutdown of state Route 109 near Ocean City along the central coast, department spokeswoman Lisa Murdock said.
Source: http://www.energycentral.com/sections/newsroom/nr_printer_friendl y.cfm?id=3549320

5. *January 04, BBC* — **Two breakdowns at Russian nuclear power stations in 24 hours. There have been two emergencies at once over the past 24 hours at nuclear power stations in Russia.** During the day yesterday a short circuit caused one of the generators of the second energy unit at the Smolensk [western Russia] nuclear power station to switch off. The unit is currently working at 50 per cent of its capacity. Also, the automatic security system went into motion at the second energy unit of the Kalinin nuclear power station [north of Moscow] this

morning. It has been switched off temporarily. **The cause is being investigated. Staff members say radiation levels at the stations do not exceed the normal background level.** No violations of safety procedures have been established.
Source: http://www.energycentral.com/sections/newsroom/nr_article.cfm?id= 3549252

6. *January 03, PR Newswire* — **Power plant construction hits record year. More than 54,000 megawatts of new U.S. power generation were completed in 2002, a record year for construction despite the ongoing financial problems at many energy companies,** according to Energy Argus analysts. The 54,019 MW is about three−quarters of the plants expected to come online last year, showing the impact of spending cuts at some utilities. **Nearly all the plants are fueled by natural gas, which is capturing a growing share of the electric generation fleet.**
Source: http://hsweb01.screamingmedia.com/PMA/pma_newsarticle1_national.h tm?SMDOCID=comtex_2003_01_03_pr_0000−1999−.industrytopstories.uti la>

[Return to top]

Chemical Sector

Nothing to report.
[Return to top]

Defense Industrial Base Sector

7. *January 06, Aviation Week &Space Technology* — **Military Satcom, relay programs boost industry, enhance warfare.** About 20 large military communications and secret National Reconnaissance Office relay spacecraft worth $3−4 billion are under development for launch over the next 10 years, giving a much needed stimulus to satcom developers and enhanced data and network−centric capability to the U.S. in a dangerous world. **Unmmaned Aerial Vehicles (UAVs) and network−centric operations are a primary reason the Defense Dept. earmarked $3 billion starting in Fiscal 2003 for the satcom Transformational Communications program,** said Kevin Meiners, the director of intelligence, surveillance and reconnaissance systems under the assistant secretary of defense for command control communications and intelligence. "We do not want UAV operations limited by bandwidth," he told a UAV conference near Orlando, Fla., recently. **While the commercial satcom business is down, military and other government−related satcom and relay business is on an upswing and about to overtake the commercial sector in overall development activity,according to Alexis C. Livanos, executive vice president of Boeing Satellite Systems. Over the next several years, the military satcom and other more classified NRO relay work may account for roughly 60% of the satcom−related U.S. developments, turning the tables on the period through the 1990s when commercial satcoms dominated.**
Source: http://www.awstonline.com/cgi−bin/authenticate.pl?destination=doc s/issues/20030106/aw43.htm

[Return to top]

Banking and Finance Sector

Nothing to report.

[Return to top]

Transportation Sector

8. *January 06, Washington Post* — **Armed man seized after hijacking in Germany. An armed man seized a single–engine aircraft from an airfield southeast of Frankfurt Sunday afternoon and threatened to crash into the European Central Bank as he circled above the city's financial center, police said.** He landed safely two hours later. While two military jets and a police helicopter shadowed the plane, the hijacker told officials and journalists in contact with him by radio and cellular phone that he wanted to draw attention to one of the astronauts killed in the 1986 Challenger space shuttle disaster in the United States. Police arrested the 32–year–old man, a student, after he landed at the city's international airport, **ending a drama that shut down continental Europe's busiest airport and Frankfurt's railway station and led to the evacuation of all high–rises in the city center. Although the military jets following the plane were armed, the German government has no legal mechanism that allows the chancellor, or any other government official, to order a hostile civilian aircraft to be shot down, officials said.** The government recently set up an airspace security working group to examine the issue and make legislative recommendations to allow such an action.
Source: http://www.washingtonpost.com/wp–dyn/articles/A14409–2003Jan5.htm l

9. *January 06, Aviation Week &Space Technology* — **TSA meets goal with cast of thousands.** The Transportation Security Administration rang in the New Year by moving to 100% screening of all checked baggage for explosives as mandated by Congress, but the agency doesn't expect to achieve all–electronic screening until later this year. In the meantime, K–9 teams with dogs to sniff out explosives as well as hand searches will be used at times in conjunction with "positive passenger bag match" to make sure no bag gets on an aircraft without being screened, according to former Coast Guard Commandant James M. Loy, the leader of the Transportation Security Administration. The Dec. 31 baggage screening mandate was the final one of 36 set by Congress. All were met by TSA, including the Nov. 17 deadline for screening passengers. **Loy said TSA employed more than 105,000 people in the field to meet the deadline, including 41,000 temporary contractors and 66,000 new TSA employees.** About 1,000 of these TSA personnel are Washington–based. Since Congress set a cap of 45,000 for permanent TSA employees, 21,000 of those hired by TSA are on temporary status. **TSA's workforce of 56,000 screeners breaks down to 33,000 checking passengers and 23,000 checking baggage. In all, 1,100 new EDS CAT–scan machines and 5,600 explosive trace detection machines have been installed.** Fifty more EDS machines may be purchased in Fiscal 2003 and airports could elect to buy additional machines on their own if they deem it necessary.
Source: http://www.awstonline.com/cgi–bin/authenticate.pl?destination=doc s/issues/20030106/aw35.htm

10. *January 05, Associated Press* — **No delays reported in baggage screening system.** Around the country, air travelers had a postitive impression of what was expected to be the heaviest

travel day since January 1, when a Congressional order went into effect requiring that every checked bag at more than 400 of the nation's commercial airports be screened for explosives. **Spot checks Sunday at several of the nation's airports showed no major delays caused by the new security measures.** At the international terminal for Northwest Airlines at John F. Kennedy International Airport in New York, passengers waited up to 30 minutes longer than usual while their bags were sent through giant screening machines and workers ripped open taped boxes and rifled through their contents before closing them up again. **Before the attacks of September 11, 2001, only 5 percent of the roughly 2 million bags checked each day were screened for bombs.** The federal government put an additional 23,000 screeners into airports to implement the new order that no checked bag be allowed through without verification that it contains no explosives.
Source: http://www.cnn.com/2003/TRAVEL/01/05/baggage.screening.ap/

11. *January 03, U.S. Department of Transportation* — **Federal Transit Administration launches emergency preparedness forum in Hartford, CT. Federal Transit Administrator Jennifer L. Dorn will open the Federal Transit Administration's (FTA) "Connecting Communities: Emergency Preparedness and Security Forum" in Hartford on Jan. 8–9. The forums were created to help communities become better prepared to respond to emergency situations.** Using the successful evacuation of the transit stations below the World Trade Center on Sept. 11, 2001 as a benchmark, the goal of the forums is to demonstrate the important role that transit plays in crisis situations and the importance of delivering a coordinated regional response to any emergency. Participating transit agencies will work with regional emergency responders to determine the effectiveness of interagency response plans for the Hartford region. The forums, which will continue in other U.S. cities through early 2003, have been created in cooperation with FTA's partners, the American Public Transportation Association and the Federal Railroad Administration. The FTA has been working with the Connecticut Transit System (CT Transit) to host the forum. **FTA's five–part Security Initiative includes evaluating threats and vulnerabilities through a security assessment; developing a plan to address vulnerabilities; testing the plan in realistic situations; training employees to understand and implement the plan; and undertaking research to enhance human capabilities. Future scheduled forums are Jan. 22–23 in Newark, NJ; Feb. 5–6 in Los Angeles; and Feb. 26–27 in San Diego.**
Source: http://www.dot.gov/affairs/fta0103.htm

[Return to top]

Postal and Shipping Sector

12. *January 03, Wall Street Journal* — **U.S. rule may impede cargo from Hong Kong. Goods headed to the U.S. from the world's largest container port could face costly delays as Hong Kong's shipping industry struggles to comply with strict U.S. Customs Service rules aimed at combating terrorism. Industry officials say Hong Kong is unprepared to comply with a new rule, put in place Dec. 2 with a 60–day grace period, that requires ports to provide comprehensive details of shipping containers 24 hours before a vessel departs for a U.S. port.** Under the old rules, less–detailed cargo data could be sent to U.S. officials up to two weeks after a ship had set sail. "The shippers are not ready, we are not ready. It's as simple as that," said a spokeswoman for the Hong Kong Association of Freight Forwarding and

Logistics. Vessels failing to meet the new requirement could be detained at their port of origin. **With more than a million tons of goods heading by sea to the U.S. every month, even a slight delay at the dock could cause trouble for manufacturers and retailers in the U.S.** In October, a 10–day shutdown of West Coast ports led to a costly backlog of containers at Hong Kong terminals that took weeks to set right. **Hong Kong is crucial to U.S. efforts to expand its security focus abroad. It ranks as world No. 1 in number of cargo containers shipped to the U.S.**
Source: http://online.wsj.com/article_email/0,,SB1041535327911860433,00.h tml

[Return to top]

Agriculture Sector

13. *January 05, Observer (UK)* — **Bioterrorists may mount foot and mouth attack.** Following recent warnings that terrorists are planning a high street attack, attention has moved to another potential target – the national herd. **Ministers will launch their animal welfare strategy on Wednesday, starting plans for a 10–year 'biosecurity' operation to protect livestock.** Safeguarding the economy and food chain from the deliberate introduction of livestock viruses has become a pressing concern. **Neil Thornton, director of animal health for the UK Department of the Environment, Food and Rural Affairs, said the threat of bioterrorism had become a "legitimate area for us to cover."** The devastating impact of the last foot and mouth outbreak underlined its potency as a potential weapon. Defense experts believe foot and mouth could be a low–tech weapon of mass destruction. Not only can the disease be produced on a huge scale, it can also be transported without detection in a container the size of a fountain pen. **A surveillance scheme designed to increase early detection of disease in the national herd and prevent viruses entering the UK will be devised in tandem with the welfare strategy.**
Source: http://politics.guardian.co.uk/homeaffairs/story/0,11026,868990,0 0.html

14. *January 04, Omaha World–Herald* — **Vaccine promising in E. coli fight. University of Nebraska (NU) researchers, in collaboration with their Canadian counterparts, may have found a way to reduce deadly E. coli bacteria in cattle. NU researchers have learned that cattle treated with an experimental vaccine developed in Canada release significantly less E. coli O157:H7 in their waste, indicating that the E. coli was killed.** The Nebraska research indicates that the incidence of E. coli can be further reduced by supplementing cattle feed with a beneficial bacteria that keeps E. coli from attaching to cattle intestines. In research last summer at UNL's test feedlot at Mead, the vaccine was more effective than the feed supplement when the two were tested separately. The reduction in E. coli was most dramatic when the two were used together, according to Moxley. **The NU research is the first to focus on how E. coli O157:H7 gets into animals on the farm. Up to now, the problem of contamination has been tackled at slaughtering plants.** The development could someday spare Americans the sickness caused by E. coli O157:H7 in meat and reduce the economic risk of beef recalls.
Source: http://www.omaha.com/index.php?u_np=02115

[Return to top]

Food Sector

15. *January 04, Associated Press* — **New York company recalls chicken hot dogs. A New York–based company is recalling 26,400 pounds of chicken frankfurters because they may be contaminated with harmful bacteria. The frankfurters made by PRG Packing Corp. may be contaminated with listeria, which can cause food poisoning.** The meat was produced on November 27 and distributed to stores and wholesalers in Connecticut, Massachusetts, New Jersey and New York. So far, no illnesses have been reported. Listeria can cause a severe, flu–like illness and, in some cases, death. People who are prone to infection include those with weak immune systems, the elderly, children, and pregnant women.
Source: http://www.theithacajournal.com/news/stories/20030104/localregion al/707415.html

[Return to top]

Water Sector

Nothing to report.
[Return to top]

Public Health Sector

16. *January 06, Sunday Mirror (UK)* — **New dye identifies bacteria. Scientists have developed a hand–cream which exposes the presence of potentially lethal bacteria such as Methicillin Resistant Staphylococcus Aureus (MRSA) on doctors' and nurses' hands.** The new cream contains a dye that exposes the bacteria found commonly in hospitals. Under ultra–violet light, clean areas of skin on the hand appear purple while contaminated patches show up white. **So successful is the test that Huddersfield Royal Infirmary has seen a 30 percent drop in infections on its surgical wards, and the initiative is being applied across the UK.** Dr Anne Marie Seeney, head of infection control at Huddersfield, said: "We know that 10 per cent of all patients will pick up an infection in hospital and we have been able to reduce that to about seven per cent."
Source: http://www.sundaymirror.co.uk/homepage/news/page.cfm?objectid=125 02947iteid=81959

17. *January 06, Sun Sentinel* — **100 sick on trip to Caribbean, cruise line says. About 100 passengers reported various stages of a stomach flu on the Norwegian Cruise Lines ship Norway, said company spokeswoman Susan Robison.** The ship, carrying 2,200 passengers, docked at the Port of Miami on Sunday morning after a seven–day eastern Caribbean cruise. **The outbreak is the latest flu–like illness, including the Norwalk virus, to hit a string of cruise ships in the past few months.** While some cruise lines canceled sailings and offered refunds, the financial effect has been minimal so far, according to financial analysts. **Industry watchers are waiting to see how the wave of illnesses affects bookings as the traditionally highest sales period of mid–January through February begins.**
Source: http://www.sun–sentinel.com/news/local/palmbeach/sfl–pccruise06ja n06,0,3093187.story?coll=sfla–news–palm

18. *January 05, Advocate* — **LSU scientists work on way to fight toxins in the body.** Antibiotics couldn't save the five Americans who died of antrax infection. That's because killing the anthrax doesn't necessarily mean the patient survives. Toxins produced by the bacteria damage the body, and a large enough dose can kill even after the anthrax is eradicated. **"There's a bunch of bacterial diseases in which the toxins are the major culprit," said Louisiana State University (LSU) biochemist Iris Lindberg. "We have a lot of ways to kill bacteria, but nothing that works against the toxins."** That is starting to change through research like Lindberg's, at LSU's Health Sciences Center in New Orleans. **She's shown in just–published results that a simple molecule, incorporating the amino acid arginine, can prevent the activation of toxins produced by the dangerous bacteria Pseudomonas aeruginosa in mice. Her antidote, called D6R, could lead to drugs that block toxins from a variety of bacteria in humans, including diphtheria, clostridium, and anthrax.**
Source: http://www.theadvocate.com/stories/010503/sci_anthrax001.shtml

[Return to top]

Government Sector

19. *January 06, Washington Post* — **Lid put on domestic spending; Bush wartime budget curbs other growth.** Under a White House budget plan that Congress will take up in the next few days, spending for domestic programs other than homeland security would be held at $316 billion in the current fiscal year –– the same as last year, according to figures provided by the House Appropriations Committee. Congressional aides expect this frugal approach to continue in the 2004 budget that President Bush will propose next month. **The policy marks a major adjustment of federal priorities in the face of soaring defense outlays, new demands for funds to protect the nation against terrorism, and stagnant tax revenue.** Spending on domestic programs funded in annual appropriations bills rose by about 40 percent in President Bill Clinton's second term, with major increases for education, natural resources, job programs, transportation and health research. **Administration officials defend the shift as essential in light of new security threats abroad and the economic downturn at home. "We've been saying for a year that the country has three big priorities: fighting terrorism abroad, protecting our homeland and ensuring economic growth. That's where you'll see money spent, and other functions of government will have to grow more slowly than in previous years. We can't make the mistakes of trying to have guns and butter," said Amy Call, a spokeswoman for the White House budget office.**
Source: http://www.washingtonpost.com/wp–dyn/articles/A14741–2003Jan5.htm l

20. *January 06, Inside the Air Force* — **Pentagon budgets for at least two more years of combat air patrols.** The Pentagon plans to allocate nearly $800 million during the next two fiscal years to continue flying combat air patrols –– Air Force jets flying to protect domestic air space, according to Pentagon sources. **In fiscal year 2004, which begins in October of 2003, the Air Force is expected to use about 46,000 flying hours for the CAPs, according to program budget decision No. 203R, dated Dec. 12. Pentagon Comptroller Dov Zakheim signed the "for official use only" document, which adjusts funding for active Air Force operations accounts.** The Air Force's budget estimate for FY–04 and beyond, submitted to the Office of the Secretary of Defense in September, lacked funding for the effort, according to the PBD. **However, OSD has added to the service's topline to continue the operations. The Air**

Force will receive $394 million in FY−04 and another $401.1 million in FY−05 to continue supporting the CAPs, the PBD says.
Source: http://ebird.dtic.mil/Jan2003/s20030106144157.html

21. *January 06, Associated Press* — **Deadline looms for foreign students to register with INS.** By Jan. 30, campuses nationwide must be prepared to submit to the INS information about their international students via the Internet−based system known as the Student and Exchange Visa Information Service, or SEVIS. **While the INS already requires the information from students and their schools, SEVIS −− which was up and running as of Jan. 1 −− will replace the cumbersome paper−based system that the INS has used for years to keep track of international students. In the past, school kept the information in files, which the INS had the right to see on request.** INS spokesman Christopher Bentley says the new system is more efficient, accurate, and faster, and that students needn't worry about the kind of fears that Zuberi cites.
Source: http://www.thebostonchannel.com/news/1870226/detail.html

[Return to top]

Emergency Services Sector

22. *January 05, New York Times* — **Police departments scramble to make patrol cars safer.** With serious questions raised about the safety of the Crown Victoria, the Ford sedan that is popular as a police patrol car, the New York Police Department and other major police forces in the metropolitan region are scrambling to make their Crown Victoria cruisers safer. Concern about the model's safety has grown since Dec. 19, when a Crown Victoria patrol car used by a state trooper was struck from behind on the New York State Thruway in Yonkers and burst into flames, killing the trooper and two other people. **Some troopers blamed the fire on the Crown Victoria's oddly−positioned gas tank and refused to drive their cruisers until the tanks were equipped with protective shields. In September, Ford officials began notifying police departments across the country that the company would provide and install shields free in all Crown Victoria cruisers.**
Source: http://www.nytimes.com/2003/01/05/nyregion/05VIC.html

[Return to top]

Information and Telecommunications Sector

23. *January 07, Computerworld* — **Think Tank says the threat of cyberterrorism is overrated.** A research paper released last month by the **Center for Strategic &International Studies (CSIS), a Washington−based Think Tank, argues that computer networks and critical infrastructures are distinct entities and that the threat from cyberterrorism is far less serious than the government and the media contend.** "While many computer networks remain very vulnerable to attack, few critical infrastructures are equally vulnerable," argues James A. Lewis, a CSIS analyst. **"Computer network vulnerabilities are an increasingly serious business problem, but their threat to national security is overstated."** However, Brenton Greene, deputy director of the National Communications System, an executive−branch

agency responsible for maintaining and restoring communications during times of national crisis, said the **physical and cyber aspects of critical infrastructure protection can't be separated. Major physical events will have digital ramifications** and vice versa, said Greene. That's also the conclusion of the recently released annual report of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, led by former Virginia Governor James S. Gilmore. **"Cyberspace has been isolated and specialized, thus limiting its perceived relevance to day–to–day outcomes and even its relevance to what are viewed as clear and present homeland security threats,"** the commission stated.
Source: http://www.computerworld.com/securitytopics/security/cybercrime/story/0,10801,77239,00.html

24. *January 06, Federal Computer Week* — **Army considers urban warfare technology. The Army's Intelligence and Information Warfare Directorate (I2WD) is reviewing responses to a recent request for information (RFI) for technology that can be used to gather intelligence and fight enemy forces in an urban environment.** However, this type of battle, especially in a foreign city, poses **numerous problems for the Army, not the least of which is quickly identifying "bad guys" as opposed to innocent civilians,** said Fran Orzech, chief of I2WD's information operations technology development branch at Communications–Electronics Command (Cecom) in Fort Monmouth, N.J. That task is made even more difficult when **enemy forces set up command and control (C2) centers using commercially available communications equipment in hospitals, schools and other locations where innocent city workers and inhabitants can also be found,** Orzech said. The **"sheer density of radio frequency signals" in an urban environment, emitted from those commercial systems as well as wireless and paging systems, is yet another complicating factor,** he added. The RFI is part of a new four–year, science and technology objective program – Information Operations for the Objective Force –that is focused on maturing sensor technology, signal processing techniques and computer network operations for transition to the Army's Future Combat Systems (FCS) and other transformational programs.
Source: http://www.fcw.com/fcw/articles/2003/0106/web–cecom–01–06–03.asp

25. *January 06, New York Times* — **Experts see vulnerability as outsiders code software. As American companies increasingly move their software development tasks out of their own offices to computer programming companies here and abroad,** new concerns are being raised about the security risks involved. The companies providing outsourcing services say that they take all necessary precautions to limit risk. But **the question of whether the booming business in exporting high–tech jobs is heightening the risk of theft, sabotage or cyberterrorism from rogue programmers has been raised in discussions at the White House, before Congress and in boardrooms.** "I can't cite any examples of this happening – but what that means is we haven't found any," said James Lewis, director of the technology program at the Center for Strategic and International Studies in Washington. While operations in some countries, like the United States, Britain and India, are considered generally safe for such software outsourcing, **nervousness is beginning to grow at companies and in the government about the possibility of abuse by hackers, organized crime agents and cyberterrorists in nations like Pakistan, the Philippines and Russia.** It is easy to see why companies find the economics of outsourcing compelling; **cost savings can be 25 to 40 percent.** Forrester Research of Cambridge, Massachusetts, predicted in a recent report that the **acceleration in outsourcing would result in 3.3 million American jobs' moving offshore by**
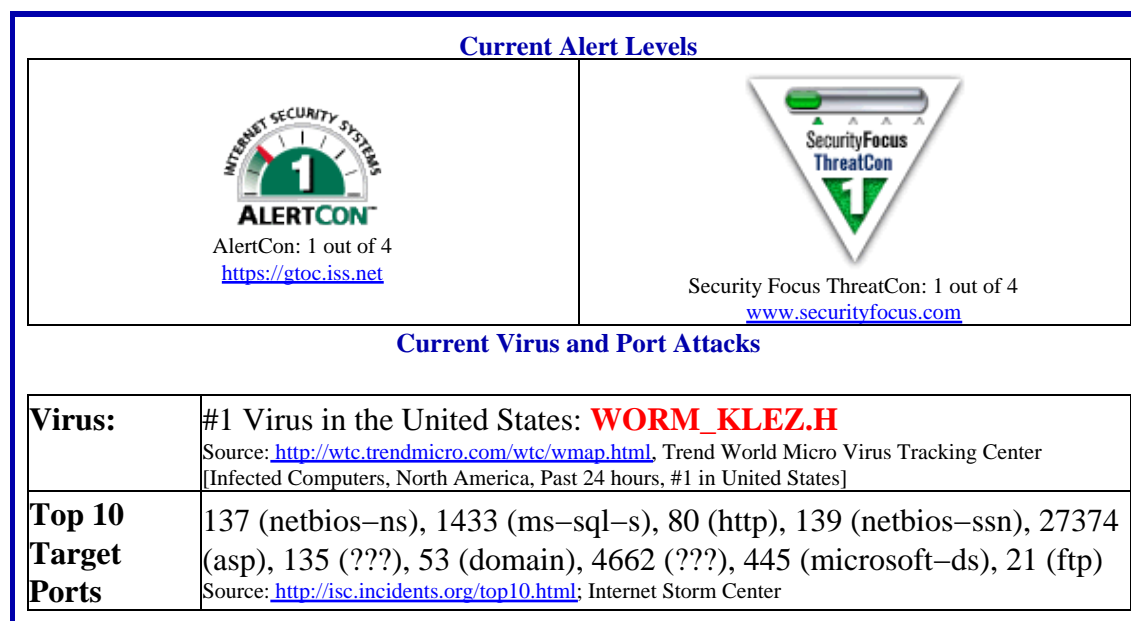
2015. Forrester estimates that **70 percent of these jobs will move to India, 20 percent to the Philippines and 10 percent to China.**
Source: http://www.nytimes.com/2003/01/06/technology/06OUTS.html

26. *January 06, Washington Post* — **Setting up IT infrastructure will help the Department of Homeland Security.** One of the challenges in creating a department from a hodgepodge of 22 federal agencies and 170,000 employees is the information technology headache. "It is not enough to shuffle redundant or overlapping programs under the new bureaucracy," Michael Scardaville, a policy analyst at the Heritage Foundation, wrote in a recent report. **The department "should develop and deploy an information technology infrastructure that links and fuses intelligence and law enforcement terrorism databases.**" Representative of the agency's challenge will be monitoring the thousands of freighters that enter U.S. ports daily. **The department wants a "smart border" program in which cargo ships heading for U.S. ports would electronically file information detailing the contents of cargo containers, crew members' names and nationalities, and what stops the ships are scheduled to make before reaching the United States.** Steven I. Cooper, special assistant to the president on information technology's place in homeland security, admitted, it may be a lengthy process. "I think parts of it could probably be done fairly quickly, meaning within months instead of years," he said. "To fully put together something like that across the world is obviously going to take a longer period of time." In the meantime, **short term priorities for the new department will include border and transportation security technology, such as equipment that identifies radioactivity and software that identifies non−obvious trends in databases or protects computer infrastructure from hackers.**
Source: http://www.washingtonpost.com/wp−dyn/articles/A11573−2003Jan4.htm l

Internet Alert Dashboard

Current Alert Levels	
AlertCon: 1 out of 4 https://gtoc.iss.net	Security Focus ThreatCon: 1 out of 4 www.securityfocus.com

Current Virus and Port Attacks	
Virus:	#1 Virus in the United States: **WORM_KLEZ.H** Source: http://wtc.trendmicro.com/wtc/wmap.html, Trend World Micro Virus Tracking Center [Infected Computers, North America, Past 24 hours, #1 in United States]
Top 10 Target Ports	137 (netbios−ns), 1433 (ms−sql−s), 80 (http), 139 (netbios−ssn), 27374 (asp), 135 (???), 53 (domain), 4662 (???), 445 (microsoft−ds), 21 (ftp) Source: http://isc.incidents.org/top10.html; Internet Storm Center

[Return to top]

General Sector

27. *January 06, Associated Press* — **Team readies 3–D models of landmarks in case of attack. A team of architecture experts says its digitized model of the Statue of Liberty could be used to rebuild the national landmark if it is damaged or destroyed in a terrorist attack.** Using a high–tech laser scanner to measure its surface from all angles, the team from Texas Tech University has been working for nearly two years to create computerized, three–dimensional drawings of the monument. Officials with the National Park Service, which administers the statue, called on the team to create the model it says could help create an accurate replica if any section of it were ever destroyed, the Daily News reported in its Sunday editions. Mount Rushmore has also been scanned into three–dimensional images, and the U.S. Capitol in Washington, D.C., underwent computer scanning in the days after the Sept. 11 terrorist attacks, the Daily News reported. **The computer images of the Statue of Liberty are especially important. Her creator left no blueprints and only minimal design sketches, so replacing her in the event of a catastrophic loss would have been all but impossible.**
Source: http://www.suntimes.com/output/terror/cst–nws–threed06.html

28. *January 06, Washington Post* — **Double bombing kills 22 in Israel.** Two Palestinian bombers blew themselves up a block apart in a busy immigrant neighborhood here tonight, killing at least 22 people and injuring an estimated 108 others in the deadliest attack in Israel in more than nine months, according to police officials. **The suicide bombers set off the explosions within a few seconds of each other in an area of mostly foreign workers, near the sites of two suicide bombings last year.** The force of the coordinated explosions at 6:30 p.m., the first near a bus stop, the second on a pedestrian mall, turned a busy workday evening into a scene of carnage, flinging body parts more than 100 feet from the blast sites, blowing out plate–glass windows 300 feet away and sending hundreds of screaming shoppers, commuters and residents scrambling for cover. **The al–Aqsa Martyrs Brigades, a militant group linked to Palestinian leader Yasser Arafat's Fatah movement, asserted responsibility for the bombings and said they were retribution for the destruction of Palestinian homes by Israeli forces. A statement released to the Arab satellite television network al–Jazeera identified the two bombers as Boraq Halfa and Saver al–Nouri, both from the West Bank city of Nablus, about 35 miles northeast of Tel Aviv.**
Source: http://www.washingtonpost.com/wp–dyn/articles/A16490–2003Jan6.htm l

29. *January 06, Associated Press* — **Terror suspects agree to extradition to U.S.** Two Pakistanis and an Indian–born U.S. citizen told a court Monday they would not fight extradition to the United States on charges of plotting to trade drugs for anti–aircraft missiles that they planned to sell to the al–Qaida network. **Authorities had expected a protracted legal battle, and their defense lawyer said he was surprised by his clients' decision. Authorities accused the men of offering hashish and heroin for four shoulder–fired Stinger missiles that could be used to attack low–flying civilian jetliners or military aircraft.** Syed Saadat Ali Faraz, 54, and Muhammed Abid Afridi, 29, both of Peshawar, Pakistan, and Ilyas Ali, a 55–year–old American citizen from Minneapolis, have been jailed since their arrest. The men did not say why they were willing to be handed over to the United States where face life in prison if convicted. **The three were arrested on Sept. 20 by Hong Kong police working together with the FBI.**
Source: http://www.nytimes.com/aponline/international/AP–Hong–Kong–Terror–Suspects.html

NIPC Products &Contact Information

The National Infrastructure Protection Center (NIPC) serves as a national critical infrastructure threat assessment, warning, vulnerability, and law enforcement investigation and response entity. The NIPC provides timely warnings of international threats, comprehensive analysis and law enforcement investigation and response. The NIPC provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the NIPC web−site (http://www.nipc.gov), one can quickly access any of the following NIPC products:

NIPC Advisories – Advisories address significant threat or incident information that suggests a change in readiness posture, protective options and/or response.

NIPC Alerts – Alerts address major threat or incident information addressing imminent or in−progress attacks targeting specific national networks or critical infrastructures.

NIPC Information Bulletins – Information Bulletins communicate issues that pertain to the critical national infrastructure and are for informational purposes only.

NIPC CyberNotes – CyberNotes is published to support security and information system professionals with timely information on cyber vulnerabilities, malicious scripts, information security trends, virus information, and other critical infrastructure−related best practices.

NIPC Daily Open Source Report Contact Information

Content and Suggestions:	Melissa Conaty (202−324−0354 or mconaty@fbi.gov)
	Kerry J. Butterfield (202−324−1131 or kbutterf@mitre.org)
Distribution Information	NIPC Watch and Warning Unit (202−323−3204 or nipc.watch@fbi.gov)

NIPC Disclaimer

The NIPC Daily Open Source Report is a daily [Monday through Friday] summary and assessment of open−source published information concerning significant critical infrastructure issues. This is an internal NIPC tool intended to serve the informational needs of NIPC personnel and other interested staff. Further reproduction or redistribution for private use or gain is subject to original copyright restrictions of the content. The NIPC provides no warranty of ownership of the copyright, or of accuracy in respect of the original source material.